STATEMENT OF SENATOR TOM COBURN
Chairman, Subcommittee on Federal Financial Management, Government Information and International Security
July 28, 2006

Welcome to today's hearing titled "Cyber Security: Recovery and Reconstitution of Critical Networks." This is the second hearing in a series we will be conducting on cybersecurity. On July 19, 2005, this Subcommittee held a hearing on the importance of cybersecurity to our nation's critical infrastructures. The hearing highlighted the importance of forging a public/private partnership to protect critical infrastructures and focused on challenges facing the Department of Homeland Security (DHS) in facilitating and leveraging such a partnership. Important lessons learned through the September 11 terrorist attacks and the response to Hurricane Katrina further emphasized these challenges. Today, despite spending millions of dollars over the past year, DHS continues to struggle with how to effectively form and maintain effective public/private partnerships in support of cybersecurity—including how to protect Internet infrastructure and how to recover it in case of a major disruption. The public/ private partnership necessary to

accomplish DHS's goals in securing computer networks continues to remain a public/ private divide. I am grieved to note that our Nation's security from a cyber based attack has not improved since we were here last year. The objective of today's hearing is to highlight immediate steps that DHS and the private sector can take to formalize a partnership and to ensure effective response and recovery to major cyber network disruptions.

Our economy and national security are reliant on the Nation's information and communications infrastructure including the Internet. The Internet connects millions of information technology systems and networks together, which, in sum, provide e-commerce to the country and critical services allowing the government to function. July 19, 2005, we learned that these computer networks can also control physical infrastructure such as electrical transformers, chemical systems, and pipelines. DHS recently released its National Infrastructure Protection Plan (NIPP)—almost three years late. This plan highlights the

importance of cybersecurity and the Internet to critical infrastructure, stating that the U.S. economy and national security are highly dependent upon the global cyber infrastructure, but according to today's GAO report DHS fails to adequately plan for recovery of key Internet functions. Moreover, the department has not adequately prepared to effectively coordinate public/ private plans for reconstitution from a cyber internet disruption. The success of the protection efforts in the NIPP hinges on information sharing between the federal government and the private sector. However, a number of barriers exist to information sharing. Recent incidents at the Department of Veterans Affairs, Department of State, and a National Laboratory indicate that the government has trouble protecting sensitive information. The government also does not have a good record of sharing sensitive intelligence-derived threat data with the private sector.

GAO identified numerous challenges to development of a plan and is here today to present their recommendations to strengthen the

department's abilities. Government agencies and private companies, including telecommunications companies, cable companies, peering organizations and major data carriers, need clarity on what is expected of them in a crisis. Overlapping and unclear roles and responsibilities lead to frustration and confusion, and will hamper recovery efforts in a crisis.

The overarching concern for the Committee is whether the Department of Homeland Security knows what functions of government need to be protected, how those functions interact with state and local governments, and what is DHS's role and responsibility in working with the private sector during a cyber or telecommunications based incident of national significance? The recently released DHS plan requires the use of a risk assessment method that has been criticized as not focusing on what really needs to be protected in the information technology and telecommunications sectors, and focusing heavily on physical assets. The risk assessment methodology should be reevaluated as

it could lead to wasteful spending. While this sector has physical assets to protect, government needs to understand that this sector is about protecting critical functionality. The private sector and government must work together to ensure the nation's critical infrastructure can function in the reliable and stable fashion the American public expects. Therefore private industry must devise plans in coordination with the government to ensure critical functions do not fail or can be recovered quickly when faced with an incident of national significance – like Hurricane Katrina. The National Communications System has worked under this concept for years.

Both government and private industry admit that there are vulnerabilities in the networks that can and have been exploited or damaged by accident or by natural causes—a perfect system cannot be built. The difficult part for any organization, especially government, is how does it respond, recover and reconstitute after an incident. The Homeland Security Act of 2002 and presidential

directives lay out a clear mandate on cybersecurity at the Department of Homeland Security. They require DHS to 1) assess our vulnerability to cyber attack 2) develop a plan to fix it and 3) implement that plan using measurable goals and milestones. In order to implement the plan the Department has the admittedly difficult task of engaging and securing action from diverse players including state and local governments, other federal agencies, and, especially, key industry actors. The nature of terrorists is to attack private citizens as we recently saw in the horrific railway attacks in India. There can be no excuse for not effectively engaging the private sector, even though it is hard. We ask no less of our food safety, airline security and pharmaceutical industries. The issue is lack of leadership and courage.

Nobody wants to micromanage the private sector or DHS; however, America expects DHS and the private sector to take every reasonable measure to protect us from terrorism. I am not convinced that threshold has been met.

If America is to be safe from the damage of a cyber attack, we will need a plan, a budget tied to that plan, and Congressional commitment to the implementation of the plan. One year ago, the Department announced the creation of the position of Assistant Secretary for Cyber and Telecommunications Security to elevate the importance of cyber critical infrastructure protection. Today this position remains vacant. This vacant post was designed by the Department to lead the Nation in buttressing our critical information technology and telecommunication systems against threats. The Department, working in conjunction with the private sector, needs to find that person and set that person to the task of reforming the plan and then implementing. A leader can and will be found and I encourage DHS to exhaust every effort to fill this position, ensure the proper authorities are in place to succeed, and ensure that this person receive adequate support from the top leadership at DHS to fulfill the mission.

To that end, I look forward to hearing from our witnesses from DHS, NSA, OMB, GAO, AT&T, VeriSign, Internet Security Systems and the Business Roundtable.